



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

400572740000002098
BARRINGTON AMBULANCE DEPARTMENT EMS
41 PROVINCE LANE
BARRINGTON NH 03825

April 25, 2022

Dear Barrington Ambulance Department Ems:

Comstar, LLC ("Comstar") writes to make you aware of a security incident that may affect the security of certain individuals related to Barrington Ambulance Department Ems. To date and after thorough investigation, we have no evidence that your data was subject to unauthorized access. However, since the possibility exists, we are writing out of an abundance of caution to provide this notice and inform you of the steps we are taking in response.

On or about March 26, 2022, Comstar discovered suspicious activity related to certain servers within its environment. We immediately took steps to secure our network, and launched a thorough investigation, with the assistance of third-party experts, to determine the nature and scope of the incident. Through the investigation, we determined that Comstar was the subject of a cyber-attack that impacted our network. The investigation determined that certain files on our network were subject to unauthorized access. As such, we conducted a comprehensive review of the potentially impacted files to determine what information was contained therein and to whom it related. When this review was completed, we immediately began a subsequent review of the results to identify address information for the individuals whose information may have been affected and to determine to which organization the individuals relate. This additional review confirmed that individuals related to Barrington Ambulance Department Ems were potentially impacted. The information that may have been impacted by this incident includes information within the PCR report including name, date of birth, medical assessment and medication administration, health insurance information, and Social Security number.

The confidentiality, privacy, and security of information in our care is one of our highest priorities, and we have strict security measures in place to protect information in our care. When we discovered this incident, we immediately reset the account passwords and took steps to determine what personal, confidential, and client data might be at risk. While we had policies and procedures in place at the time of the incident regarding security of information, we are reviewing those existing policies and procedures to further protect against similar incidents moving forward. We are also investigating additional security measures to mitigate any risk associated with this incident and to better prevent similar incidents from occurring in the future.

Your organization may have certain legal duties in response to this matter, including providing notice of this incident to those affiliated with your organization whose information may have been impacted, and we recommend you share this letter with legal counsel. Your organization may have contractual notice obligations, as well.

In order to minimize the impact on your business, Comstar will provide notice of this event to those affected individuals affiliated with your organization on your behalf. A sample notice letter that these individuals would receive is attached to this letter. Additionally, Comstar is offering to take the following steps upon your request and approval:

- Mail notification letters to affected individuals affiliated with Barrington Ambulance Department Ems to explain the incident and our subsequent investigation. Please note, we will provide notice to all affected individuals for whom we have complete contact information.
- For the individuals for whom you request notification assistance, we can discuss providing these notice recipients with access to identity theft protection and credit monitoring services at no cost to them.
- Provide a toll-free telephone number to respond to individuals' questions about this incident through our dedicated assistance line.
- Notify the necessary state, federal, and international regulators, if required.

Please be advised, Comstar will not take any further action on your behalf unless written authorization to do so is provided. Upon request, we will securely send to you a list of impacted individuals associated with Barrington Ambulance Department Ems.

Please contact 877-587-4280 with any questions or concerns, available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time. If you would like Comstar to notify the individuals associated with Barrington Ambulance Department Ems and regulators, if necessary, on your behalf, please notify Comstar at 877-587-4280 no later than May 25, 2022.

We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Comstar, LLC



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Comstar, LLC, ("Comstar") writes to inform you of a recently discovered data security event that has potentially impacted the security of information <<Business Name>> provided to Comstar on your behalf. We are unable to confirm whether the information was subject to unauthorized access, but because the possibility exists, we are providing this notice. We are writing out of an abundance of caution to provide you with steps you can take to better protect yourself against the possibility of identity theft and fraud, should you feel it appropriate to do so.

What Happened? On or about March 26, 2022, Comstar discovered suspicious activity related to certain servers within its environment. We immediately took steps to secure our network, and launched a thorough investigation, with the assistance of third-party experts, to determine the nature and scope of the incident. Through the investigation, we determined that Comstar was the subject of a cyber-attack that impacted our network. The investigation determined that certain files on our network were subject to unauthorized access. As such, we reviewed the contents of those files to determine what information was contained therein and to whom it related. We are notifying you because your personal information was potentially contained in the impacted files.

What Information was Involved? This additional review confirmed that individuals related to <<Business Name>> were potentially impacted. The information that may have been impacted by this incident includes your name, date of birth, medical assessment and medication administration, health insurance information, and Social Security number.

What We Are Doing. The security of information in Comstar's care is one of our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems. While we had policies and procedures in place at the time of incident regarding security of information, we are reviewing those existing policies and procedures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. We are also reporting to regulatory officials, as required.

Although we are unable to confirm if your information was impacted, as an added precaution, we are offering you access to <<CM Length>> of credit monitoring and identity theft restoration services through [VENDOR NAME] at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to better protect against the possibility of identity theft and fraud should you feel it is appropriate to do so. You may also enroll to receive the free credit monitoring and identity theft protection services we are offering.

For More Information. We sincerely regret any inconvenience or concern this may have caused you. We understand you may have questions that are not answered in this letter. To ensure your questions are answered in a timely manner, you can call our dedicated assistance line at 877-587-4280, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

<Signatory>

<Title>

Comstar, LLC

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

Insert Potential Vendor Language

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Kentucky residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

For District of Columbia residents: the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents: the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Deutsch Kerrigan LLP is located at 755 Magazine Street, New Orleans, LA 70130.

For New Mexico residents: you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents: the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For Rhode Island residents: the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington D.C. residents: the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>.

For All U.S. residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338).